LA TECNOLOGÍA BLOCKCHAIN PARA EL ASEGURAMIENTO DE LA INFORMACIÓN DE LAS HISTORIAS CLÍNICAS EN EL SECTOR SALUD EN COLOMBIA.

OSCAR DAVID ROZO GALLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

LA TECNOLOGÍA BLOCKCHAIN PARA EL ASEGURAMIENTO DE LA INFORMACIÓN DE LAS HISTORIAS CLÍNICAS EN EL SECTOR SALUD EN COLOMBIA.

OSCAR DAVID ROZO GALLO
Ingeniero de Sistemas

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATÍCA

Ing. JOEL CARROLL VARGAS
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASÍCAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Consagro este trabajo a mis padres que a pesar de las adversidades nos han sacado adelante como personas de bien, a ellos, que con su carisma y comprensión me han apoyado en esta especialización, con voz de aliento, dedico también este logro a mi compañera de batallas Luz Novoa a mí hijo Thomas Rozo que con su llegada trajo a nuestras vidas bendiciones, junto a su mano logramos sacar este reto adelante.

AGRADECIMIENTOS

Doy gracias a mi núcleo familiar. Amistades, colegas y cómplices que me han apoyado en este proyecto también y no menos importantes las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes directa e indirectamente nos ofrecen diferentes maneras para aprender, también, a Katherine Márceles Villava a los tutores que me condujeron en la causa reconozco que sin su apoyo y dedicación éste logro no sería viable.

CONTENIDO

PÁG.

LISTA DE TABLAS

Pág.

LISTA FIGURAS

pág.

GLOSARIO

AMENAZA: Posible riesgo o vulnerabilidad que puede comprometer la seguridad, integridad o privacidad de los datos almacenados en la red.

BLOCKCHAIN: su traducción al español “cadena de bloques”, similar a un libro de contabilidad digital e inmutable, la tecnología Blockchain consiste en una red descentralizada de nodos virtuales que se interconectan entre sí. En estos nodos almacenan, validan conjuntamente datos de transacciones o eventos mediante el uso de claves cifradas.

CRIPTOGRAFÍA: son técnicas encargadas de la seguridad de la data del mundo digital usando métodos de codificación transformando los datos sensibles en mensajes indescifrables logrando con ello que sean legibles solo para aquellos con la llave adecuada.

CONFIDENCIALIDAD: concepto que define que la información de un sistema debe ser visualizada, modificada o suprimida solo por personas autorizadas para trabajar sobre la misma.

DATOS DE BASES DISTRIBUIDAS: Colección de datos correspondientes a un sistema único distribuidos en múltiples centros de cómputo de una red, conformada en sitios lógicos, conectados entre ellos, por un tipo de red de comunicaciones.

HABEAS DATA: Se conoce como el derecho que tiene un individuo para conocer, actualizar o corregir data que lo identifique y que se encuentre contenida en bancos de datos de entidades públicas o privadas

HISTORIA CLÍNICA: Conjunto de datos recolectados por la exploración física, los resultados de pruebas de laboratorio e investigación biológica y/o radiológica esta información es útil para determinar un diagnóstico, un tratamiento o pautas progresivas ante una enfermedad existente.

PACIENTE: Individuo afectado por una enfermedad que requiere tratamiento médico y cuidados específicos para su recuperación o gestión de su condición de salud

RIESGO INFORMÁTICO: afectación que se puede presentar en un sistema informático en un momento inesperado, se puede producir por una aplicación configurada de manera errada, por amenazas internas y externas, o una vulnerabilidad aprovechada por un ciberdelincuente.

SEGURIDAD INFORMÁTICA: Todo lo relacionado con informática y que se orienta principalmente a la protección de infraestructura de cómputo y lo relacionado a la información incluida en la misma.

VULNERABILIDAD: se refiere a una debilidad o fallo presente en un sistema de información que pone en riesgo la seguridad de la información y puede permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la información, por lo que resulta imperativo identificar y corregir estas vulnerabilidades con la mayor prontitud posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.[1]

[1] AMENAZA VS Vulnerabilidad, ¿sabes en qué se diferencian? [Anónimo]. INCIBE [página web]. [Consultado el 5, febrero, 2024]. Disponible en Internet: <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>.

RESUMEN

Los registros médicos son esenciales para acceder a los servicios médicos y contienen información importante de las interacciones entre médico y paciente. Estos registros médicos son esenciales para prescribir tratamientos y medicamentos y monitorear el seguimiento de enfermedades que requieren un tratamiento continuo. Sin embargo, en la era de la tecnología, la gestión de registros médicos enfrenta importantes desafíos relacionados con el almacenamiento, la transmisión y la recuperación de datos médicos.

La necesidad de superar estos obstáculos técnicos ha llevado a la búsqueda de soluciones que no sólo mejoren la eficiencia de la gestión de registros médicos, sino que también garanticen la integridad, disponibilidad y seguridad de estos datos. En ese contexto que nació la idea de utilizar la tecnología Blockchain, conocida por evitar cambios para no autorizados y garantizar la autenticidad de los registros. Esta tecnología se ha utilizado con éxito en campos como el financiero y se presenta como una alternativa prometedora al sector sanitario y sus registros médicos.

En este contexto de estos cambios tecnológicos, se extraen varias recomendaciones y conclusiones importantes:

La implementación exitosa de Blockchain en el sector salud de Colombia requiere que los profesionales de la salud y el personal administrativo adquieran las habilidades y conocimientos para utilizar la nueva tecnología. Por lo tanto, es importante brindar capacitación y educación adecuada para garantizar un uso eficaz y seguro.

La ley colombiana se centra en la protección de datos personales, por lo que se debe asegurar de su implementación, Blockchain cumple con lo establecido en la

ley de Habeas Data 1582 de 2012. Esto incluye implementar medidas de seguridad sólidas y respetar la privacidad del paciente.

La implementación de la tecnología Blockchain en la gestión de registros médicos en el sector salud colombiano representa una perspectiva innovadora para abordar los desafíos tecnológicos existentes. La implementación de la tecnología Blockchain en la gestión de registros médicos en la implementación de la tecnología en el sector de la salud brinda una oportunidad innovadora para abordar desafíos técnicos en la protección de datos. Esta tecnología ofrece una solución prometedora para transformar la forma en que se almacenan y comparten los datos, con énfasis en la integridad y la seguridad.

Recomendaciones:

El cumplimiento de la legislación colombiana: Es importante que la implementación de Blockchain para la gestión de registros médicos cumpla con lo establecido en la Ley de habeas data 1581 de 2012. Esta ley exige estrictas medidas de seguridad y el debido respeto a la privacidad de los pacientes.

Implementar medidas de seguridad estrictas: Se recomienda que las redes Blockchain sean utilizadas para administrar registros médicos que tengan implementadas medida de seguridad estrictas. Esto incluye el cifrado de datos, controles de acceso adecuados, gestión de claves seguras y otras salvaguardas de protección para garantizar la integridad y confidencialidad de la información.

Auditorías y cumplimiento normativo: Realizar auditorías periódicas para garantizar el cumplimiento continuo de la normativa de protección de datos. Es importante garantizar que la implementación de Blockchain en los registros médicos cumpla con los estándares legales y éticos vigentes.

Capacitación y concientización: Brindar capacitación a los profesionales de la salud y al personal involucrado en la gestión de datos sobre el uso adecuado de la tecnología Blockchain, haciendo énfasis en la importancia de la seguridad y la privacidad de la información médica.

Al considerar la reciprocidad de datos médicos y la mejora en la prestación de servicios médicos que esta tecnología conlleva, se evidencia un impacto potencialmente positivo en la calidad de la atención médica y el bienestar de los pacientes.

Sin embargo, se reconoce que la implementación de Blockchain en el sector de la salud también presenta desafíos importantes, particularmente con respecto a la protección de datos personales y el cumplimiento de las leyes aplicables. Estos desafíos deben abordarse cuidadosamente de acuerdo con las regulaciones aplicable. La tecnología Blockchain, si se implementa correctamente y se superan estos obstáculos, de la tecnología puede abrir nuevos horizontes para la gestión de registros médicos y en la atención sanitaria en general.

ABSTRACT

Medical records, essential for the provision of health services, contain vital information derived from the doctor-patient interaction. These medical records are essential for prescribing treatments and medications, as well as monitoring illnesses that require ongoing care. However, in the technological era, medical record management faces considerable challenges in terms of storage, transmission, and consultation of medical data.

The need to overcome these technological obstacles has led to the search for solutions that not only improve efficiency in the management of medical records, but also guarantee the integrity, availability, and security of this data. In this context, the idea of using Blockchain technology arises, known for its ability to prevent unauthorized modifications and guarantee the reliability of records. This technology, which has found successful applications in sectors such as finance, is presented as a promising alternative for the health sector and its medical records.

In this context of technological transformation, some key recommendations and conclusions are derived:

The gradual implementation of Blockchain in the Colombian health sector is suggested, considering the critical nature of the information in medical records. This would allow for a controlled transition, minimizing potential disruptions to the flow of medical information.

The successful adoption of Blockchain in the healthcare field requires healthcare professionals and administrative staff to acquire skills and knowledge in managing the new technology. Therefore, it is essential to provide adequate training and education to ensure effective and safe use.

Given the focus on the protection of personal data in Colombian legislation, it must be ensured that any Blockchain implementation complies with the provisions of the Habeas Data Law 1581 of 2012. This includes the implementation of robust security measures and respect for the patient privacy.

Therefore, the adoption of Blockchain technology in the management of medical records in the Colombian health sector represents an innovative perspective to address existing technological challenges. This technology offers a promising solution that can transform the way medical data is stored and shared, with a focus on integrity and security.

When considering the reciprocity of medical data and the improvement in the provision of medical services that this technology entails, a potentially positive impact on the quality of medical care and patient well-being is evident.

However, it is recognized that the implementation of Blockchain in the healthcare sector also entails significant challenges, especially in relation to the protection of personal data and compliance with applicable legislation. These challenges must be addressed diligently and in accordance with current regulations. Blockchain technology, if implemented properly and these obstacles overcome, can open new perspectives in medical records management and healthcare in general.

INTRODUCCIÓN

La cuarta revolución industrial ha traído consigo una serie de tecnologías disruptivas que están impactando positivamente en varios sectores, incluyendo el de la salud. En particular, la tecnología Blockchain se destaca como una herramienta prometedora que puede revolucionar la forma en que se gestionan las historias clínicas y se interactúa con los stakeholders en el sector médico. Según una investigación en[2] su artículo "How Blockchain can Impact Healthcare: A Scoping Review," se destacan las posibilidades de ahorro de tiempo, costos y reducción de burocracia que el Blockchain ofrece en el sector de la salud.

En el ámbito de la salud, la relación médico-paciente es un componente crítico para la detección, diagnóstico y tratamiento de enfermedades. La implementación de la tecnología Blockchain para integrar historias clínicas con los stakeholders promete fortalecer esta relación. Un estudio realizado por (Hasselgren y colaboradores (2019)) en su artículo "Patients' Experiences of Accessing Their Electronic Health Records: National Patient Survey in Sweden" señala la importancia de la transparencia y el acceso del paciente a su información médica, aspectos que el Blockchain puede mejorar significativamente.[3]

La tecnología Blockchain ofrece un enfoque seguro y descentralizado para el almacenamiento y la gestión de datos médicos, lo que brinda a los pacientes y a los profesionales de la salud una mayor confianza en la integridad y la privacidad de la información. En su artículo "Blockchain for Electronic Health Records: Promising,

[2] Makhdoom, I., Abolhasani, M., & Burmeister, O. K. (2019). How Blockchain can Impact Healthcare: A Scoping Review. Journal of King Saud University - Computer and Information Sciences. DOI: 10.1016/j.jksuci.2019.01.041

[3] Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., Faxvaag, A., & Johannessen, L. (2019). Patients' Experiences of Accessing Their Electronic Health Records: National Patient Survey in Sweden. Journal of Medical Internet Research, 21(4), e12338. DOI: 10.2196/12338

But Caution Required" publicado en la revista "Oncology Nursing Forum," resaltan cómo la tecnología Blockchain puede abordar preocupaciones clave en cuanto a la seguridad y el acceso a los registros médicos.[4]

Con esta monografía se pretende realizar un análisis de la tecnología Blockchain para el aseguramiento de las historias clínicas en el sector salud por medio de una revisión bibliográfica cuyo fin es detectar el tipo adecuado para mantener reservado la integridad y la disponibilidad de la información contenida en estos documentos.

Se ha investigado en profundidad sobre los cambios que se están produciendo, cuáles son los argumentos de éxito propagados a nivel mundial y como educar a los usuarios sobre esta reciente tecnología. Los gobiernos en varios países se han involucrado con esta nueva forma de base de datos distribuida y, al observar su alto grado de confiabilidad, han comenzado a aumentar las implementaciones de Blockchain. Los procesos se vuelven transparentes, posibles de auditar y se dan a conocer bajo esta premisa.

[4] Brennan, P. F., & Bakken, S. (2019). Blockchain for Electronic Health Records: Promising, But Caution Required. Oncology Nursing Forum, 46(5), 505-506. DOI: 10.1188/19.ONF.505-506

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

A pesar de los avances tecnológicos que han marcado el ritmo de los últimos tiempos, las historias clínicas todavía presentan falencias en cuanto a su disponibilidad, confidencialidad e integridad. Por ello, las entidades tanto públicas como privadas encargadas del manejo de esta información buscan tecnologías que permitan minimizar el riesgo de la materialización de vulnerabilidades. En un mundo globalizado como el actual, es esencial que la tenga acceso a servicios de salud, tales como diagnóstico, tratamiento y prevención, de manera segura, eficiente y transparente.

Cada día se desarrollan nuevas tecnologías para aumentar la cobertura y calidad de estos servicios. La reciprocidad de información entre entidades ha demostrado beneficiar al sector salud, contribuyendo significativamente a mejorar la atención y asistencia a los beneficiarios. La adopción de estas tecnologías innovadoras se vuelve crucial para garantizar una gestión más segura y efectiva de los datos médicos, asegurando que los pacientes reciban una atención de alta calidad mientras se protege su información personal.

A hoy se puede evidenciar variados problemas procedentes de no contar con data veraz, integra y disponible. El sector salud es un tema que se investiga constantemente desde diferentes enfoques y uno de ellos es la estrecha relación que existe entre la tecnología Blockchain y la gestión de las historias clínicas, optimizando la disponibilidad, trazabilidad, confidencialidad e integridad de la información.

Las historias clínicas contienen información resultado de la atención médico – paciente y su uso es la prescripción de medicamentos o tratamiento de enfermedades que se deben detectar, tratar y manejar por el médico tratante. La necesidad de estos servicios de salud sobrelleva retos a nivel tecnológico tales como su almacenamiento, su transmisión y/o consulta, se ha detectado en los últimos tiempos la reciprocidad de esta data médica favorece al sector salud y conlleva a mejorar la prestación del servicio para el paciente; sin embargo, también se ostentan problemáticas procedentes por perplejidad referente a la integridad, disponibilidad e integridad de las historias clínicas teniendo en cuenta que para Colombia en la Ley de habeas data 1581 de 2012 se imponen disposiciones generales para la protección de datos personales.

Desde la perspectiva del habeas data, se establece que los datos personales comprenden toda aquella información asociada a una persona que permite su identificación y que es considerada sensible. Entre estos datos se incluyen aspectos como el estado de salud, las características físicas y la vida sexual, entre otros elementos que pueden formar parte de una historia clínica. La protección de estos datos es fundamental, ya que su manejo inadecuado puede comprometer la privacidad y la seguridad del individuo, siendo vital para garantizar la confidencialidad y la integridad de la información personal.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es el tipo de tecnología de Blockchain adecuada para mantener la disponibilidad, confidencialidad e integridad de la información de las historias clínicas del sector salud en Colombia?

2. JUSTIFICACIÓN

En Colombia las entidades del sector salud han presentado dificultades a nivel tecnológico por ataques cibernéticos presentados en sus infraestructuras lo anterior por vulnerabilidades detectadas por los ciberdelincuentes que buscan suplantar identidad, falsificar información, y hasta beneficios económicos por el rescate de la información hurtada, es por este motivo que a través del análisis de la tecnología Blockchain aplicada en el sector salud se reduzca este tipo de situaciones, además de volver los trámites relacionados con las historias clínicas más óptimos y confiables entre las partes interesadas al ser este un sistema encriptado donde la identificación de cada usuario sea validada por un identificador único.

La justificación para implementar la tecnología Blockchain en la gestión de historias clínicas en el sector salud de Colombia se fundamenta en la necesidad de fortalecer la privacidad y seguridad de la información médica. Las entidades de salud han enfrentado desafíos significativos debido a los constantes ataques cibernéticos que buscan explotar las vulnerabilidades en sus sistemas como lo son:

1. Cumplimiento de normativas de seguridad de la información: Normas como la ISO 27001 establecen estándares para la gestión de la seguridad de la información, que incluyen la protección de datos médicos sensibles.
2. Garantía de confidencialidad: La Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios establecen disposiciones para la protección de datos personales en Colombia, lo que refuerza la importancia de garantizar la confidencialidad de las historias clínicas.
3. Protección contra ataques cibernéticos: La Resolución 310 de 2002 del Ministerio de Salud y Protección Social de Colombia establece los lineamientos para la seguridad de la información en salud, reconociendo la importancia de proteger los sistemas de información contra ataques cibernéticos.

4. Integridad de la información: Normativas como la ISO 9001, que establece requisitos para sistemas de gestión de calidad, también son relevantes ya que garantizar la integridad de la información médica es crucial para la toma de decisiones clínicas. Estos ataques representan una amenaza grave, ya que los ciberdelincuentes intentan usurpar identidades, manipular información y, en algunos casos, obtener ganancias económicas a través de rescates por datos robados. La adopción de la tecnología Blockchain ofrece una solución innovadora al crear un sistema encriptado que valida la identificación única de cada usuario, reduciendo así la incidencia de tales amenazas y ofreciendo mayor confiabilidad en los trámites relacionados con las historias clínicas, al establecer un entorno seguro e inmutable para la gestión de datos médicos.

En el ámbito de la prestación de servicios de salud, es fundamental salvaguardar la información sensible que conforma la historia clínica de un paciente, tanto en entidades públicas como privadas. La adopción de Blockchain en este contexto garantiza la integridad, privacidad y custodia de estos datos sensibles, creando una capa adicional de seguridad que protege la información contra manipulaciones no autorizadas. Al establecer un sistema descentralizado y transparente, donde cada transacción es validada y registrada de manera segura, se fortalece la confianza de los pacientes en la gestión de sus datos médicos y se cumple con los estándares de privacidad exigidos por la legislación colombiana, como la Ley de habeas data 1581 de 2012.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar la tecnología Blockchain para el aseguramiento de historias clínicas del sector salud mediante una revisión bibliográfica con el fin de identificar el tipo adecuado para mantener la confidencialidad, integridad y disponibilidad en la información.

3.2 OBJETIVOS ESPECÍFICOS

1. Examinar los tipos de tecnología Blockchain mediante una caracterización, con el fin de establecer las funcionalidades de cada una de ellas.
2. Investigar los riesgos asociados a las historias clínicas del sector salud mediante una revisión bibliográfica con el fin de determinar el impacto que puedan tener en caso de presentarse un incidente de seguridad.
3. Establecer el tipo de Blockchain adecuado para el aseguramiento de las historias clínicas del sector salud mediante el análisis de los riesgos y funcionalidades de cada una de ellas.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La tecnología Blockchain tiene su origen en el año 2008, cuando una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto publicó el documento

técnico que describía el funcionamiento de Bitcoin, la primera criptomoneda descentralizada basada en Blockchain.[5]

El objetivo de Nakamoto era crear un sistema electrónico de pago peer-to-peer que permitiera realizar transacciones directamente entre dos partes sin necesidad de una autoridad central que validara las transacciones. Para lograr este objetivo, Nakamoto propuso la tecnología Blockchain o cadena de bloques.

En esencia, Blockchain es un registro contable distribuido que sirve como base de datos compartida para almacenar registros de transacciones. Este registro está formado por bloques encadenados criptográficamente que contienen los detalles de cada transacción, creando así un historial permanente e inmutable.

Cada bloque contiene información sobre un conjunto de transacciones y el hash criptográfico (identificador único) del bloque previo. Esto vincula los bloques y hace que la cadena sea extremadamente difícil de modificar, confiriendo un alto grado de seguridad e integridad.

Por lo que al revisar la expansión de la tecnología Blockchain ha superado el ámbito financiero y ha encontrado aplicación en diversos sectores. La reputación de seguridad y fiabilidad demostrada en las criptomonedas ha suscitado interés en diferentes áreas. Este interés ha conducido a explorar su implementación en campos más allá de las transacciones monetarias, incluyendo la industria de la salud. La atracción principal radica en el potencial de Blockchain para asegurar la integridad, confiabilidad y privacidad en el manejo de datos distribuidos, un aspecto crítico en entornos sensibles como el sector de la salud.

[5] Brennan, P. F., & Bakken, S. (2019). Blockchain for Electronic Health Records: Promising, But Caution Required. Oncology Nursing Forum, 46(5), 505-506. DOI: 10.1188/19.ONF.505-506

Así es como el Blockchain, con su enfoque en la descentralización, el cifrado y la transparencia, se está convirtiendo en una herramienta de gran interés en la gestión de información crítica y sensible, como la presente en las historias clínicas, asegurando la autenticidad y privacidad de los datos.

La tecnología Blockchain, implica una serie de elementos y conceptos que sustentan y hacen funcional en diversos contextos:

1. **Mecanismo de consenso:** Es un conjunto de reglas donde se determina el alcance de un acuerdo entre varios participantes sobre la red del estado actual de la cadena de bloques.
2. **Plataformas Blockchain:** cada plataforma tiene sus características y funcionalidades como, por ejemplo: Ethereum, Hyperledger, Corda, y EOS. dichas plataformas proporcionan herramientas para el desarrollo de Apps.
3. **Hash:** Es una función criptográfica donde se convierte en una entrada con una cadena alfanumérica de longitud fija, es unidireccional y facilita calcular el hash a partir de datos originales.
4. **Bases de datos NoSQL:** Son sistemas de bases de datos diseñados para el almacenamiento y recuperación de datos donde la estructura de las bases es racionales y tradicionales.

4.2 MARCO CONCEPTUAL

Los servicios de salud a nivel mundial son considerados uno de los servicios donde se deben cumplir con estándares que garanticen la pertinencia, oportunidad y racionalidad en las entidades prestadoras del sector**,** entendiéndose la salud como un derecho constitucional las personas que acceden a servicios en entidades ya sean públicas o privadas, deben ser conscientes que están autorizando a la entidad al manejo de información personal la cual puede llegar a ser sensible, por dicho

motivo se espera que esta sea manejada con unos altos estándares de calidad y privacidad. En este caso los prestadores de servicios de salud no solo deben brindar el servicio por el contrario también deben garantizar que sean cubiertas todas las variables en la gestión de riegos asociados a la seguridad de la información personal contenida en las historias clínicas de los pacientes.

La implementación de la tecnología Blockchain en el sector salud es un paso importante ya que esta herramienta tecnológica es lo suficientemente potente para el almacenamiento de grandes volúmenes de información, además trae consigo una seguridad adicional criptográfica desde su aparición se ha caracterizado por ser una herramienta con unos altos niveles de seguridad por su inmutabilidad.

En el contexto latinoamericano, la adopción del Blockchain se pueden analizar los siguientes conceptos:

Blockchain: Es un registro digital inmutable y descentralizado que almacena transacciones o datos en bloques enlazados criptográficamente. Cada bloque contiene un hash del bloque anterior, garantizando la integridad de la cadena. Su estructura distribuida y resistente a modificaciones ofrece transparencia y seguridad en la gestión de datos.

Criptografía: Es el conjunto de técnicas matemáticas que se utilizan para codificar y decodificar información. En el contexto de Blockchain, la criptografía de clave pública se emplea para asegurar la autenticidad y privacidad de las transacciones mediante la generación de claves pública y privada

Descentralización: Es un principio clave en Blockchain que implica la distribución de la información en una red de nodos, eliminando la necesidad de un intermediario

centralizado. Esto proporciona mayor resistencia a fallos y manipulaciones, así como transparencia en las operaciones.

Consenso: En el contexto de Blockchain, se refiere al proceso por el cual los nodos de la red validan y acuerdan la legitimidad de las transacciones. Mecanismos como Proof of Work (PoW) o Proof of Stake (PoS) garantizan el consenso y la integridad de la red[6]

Seguridad y Privacidad: La seguridad en Blockchain se logra mediante criptografía robusta y la estructura descentralizada de la red. Además, la privacidad se mantiene al ocultar la identidad de las partes involucradas en las transacciones, protegiendo la información sensible[7]

La ventaja competitiva de esta nueva tecnología es que, por sus características existe una seguridad adicional en confidencialidad, dado que la información contenida solo será accesible a través de una clave privada la cual se encuentra encriptada; además su disponibilidad es garantizada dado que la misma está replicada o distribuida en todos los nodos y por último la integridad ya que, al momento de realizarse cambios, se actualiza toda la cadena.

“El Blockchain es muy similar a la tecnología P2P (Peer To Peer), la cual permite compartir datos entre diferentes nodos. Esto significa que se puede tener la información[8] sin necesidad de centralizarla, evitando los intermediarios. Esta característica se hace útil cuando las organizaciones requieren eliminar el

[6] An overview of blockchain technology: architecture, consensus, and future trends, in: Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang (Eds.), Big Data (BigData Congress), 2017 IEEE International Congress on, IEEE, 2017
[7] “Ibid”, p. 27
[8] “Ibid”, p. 27

intermediario y no depender de ningún organismo que controle la información contenida en las bases de datos”. [9]

4.3 MARCO HISTÓRICO

Mucho antes de la aparición de la tecnología Blockchain existieron proyectos de monedad digitales criptográficas, y algunas son referenciadas en el documento técnico del Bitcoin

La primera Blockchain fue creada por una persona o un grupo de personas que se darían a conocer en el anonimato de Satoshi Nakamoto, en la actualidad la verdadera identidad sigue siendo desconocida. Fue diseñada para permitir la circulación de una moneda digital: el Bitcoin.

En el año 2008 fue presentado el documento técnico del Bitcoin a un grupo de criptógrafos el día 31 de octubre, por Satoshi Nakamoto, en una lista de correo de un movimiento de nombre Cypherpunck (rebeldes del cifrado). Relacionando un documento técnico llamado “Bitcoin: Un sistema de dinero electrónico de igual a igual”

En este documento Nakamoto estableció el concepto de Bitcoin como una “moneda digital descentralizada” dado que no hay un único administrador o entidad que tenga el control del sistema, sino que por el contrario es soportada en una red de pares (Peer-To-Peer). Una primera versión del código fue enviada por Nakamoto el 16 de noviembre de ese mismo año a algunos usuarios incluidos en la lista de difusión.

[9] Cointelegraph. (2023). Blockchain y tecnología P2P. Recuperado de https://cointelegraph.com/learn/what-are-peer-to-peer-p2p-blockchain-networks-and-how-do-they-work

El 3 de enero de 2009, el Bitcoin se puso en funcionamiento una vez fue lanzado el bloque génesis conocido como él (primer bloque del registro de transacciones) este hecho fue anunciado por Nakamoto el 8 de enero en la lista de difusión

En el año 2010 en mayo 22 se presentó lo que sería la primera compra con Bitcoin, Dos pizzas en Papa John’s las cuales tenían un costo de 25 dólares y valor pagado en Bitcoins fue de 10.000 con esta compra se consiguió calcular el valor del Bitcoin en un cuarto de centavo de dólar.

Para el año 2017 se presentó una de las más fuertes división a la red Bitcoin, Las mismas son creadas mediante cambios en las reglas de la Blockchain, cierta cantidad de nodos en la red aceptan y la otra parte no, generando una división. Los nodos compartían un historial de transacciones, luego de este cambio de reglas cada subred generada principia creando su propio historial. La primera bifurcación se dio en el mes de agosto y dio paso a la creación del Bitcoin Cash y se dio en el bloque 478558, por cada (BTC), cada propietario obtuvo 1 Bitcoin Cash (BCH) la segunda bifurcación fue el día 24 de octubre en el bloque 491407 por cada Bitcoin (BTC) un propietario obtuvo 1 Bitcoin Gold (BTG).

En el año 2021 Bitcoin rompió su propio récord y alcanzo un valor de 68,789.63 dólares. El salvador se convierte en el primer país en adoptar como divisa legal el Bitcoin. (“Bitcoin en El Salvador | "Esto no es para nosotros los ... - BBC News Mundo”).

Desde su aparición el Bitcoin no ha parado de funcionar, se espera una mayor adaptación en más países del mundo.

Figura 1 Línea de tiempo Blockchain .

Fuente: Propia

Desde aproximadamente el año 2008, la tecnología viene en expansión para incluir variedad de aplicaciones más allá de la criptomoneda. La tecnología Blockchain ha sido adoptada por empresas en todo el mundo, desde el seguimiento de la cadena de suministro hasta votaciones en línea.

Esta tecnología cuenta con un potencial al ser una herramienta poderosa cuyo fin es mejorar la seguridad, la transparencia y la eficacia en una gran variedad de industrias. a medida que la tecnología continúa evolucionando, es probable que siga siendo una fuerza disruptiva en el mundo empresarial y financiero.

4.4 ANTECEDENTES O ESTADO ACTUAL

En la actualidad esta nueva tecnología se ha dado a conocer por las criptomonedas, principalmente por la moneda virtual Bitcoin, se han oído en el día a día y en varios países. Se avanza en la creación de nuevos proyectos, el uso de Blockchain se ha extendido más allá de las criptomonedas y se aplica en áreas como la logística, la banca, la atención médica, las energías renovables y hasta la gestión de derechos de autor, entre otros. Se están explorando nuevas aplicaciones y usos, incluyendo

la creación de monedas digitales respaldadas por el gobierno y la implementación de contratos inteligentes.

En los últimos años, se ha visto un aumento en el desarrollo y la inversión de aplicaciones basadas en Blockchain. La criptomoneda, que es promovida por esta tecnología ha atraído gran cantidad de inversores y entusiastas[10]

La regulación por parte de muchos gobiernos y organismos se ha estado trabajando en políticas y marcos legales con el fin de abordar la tecnología Blockchain y las criptomonedas. Como, por ejemplo, en países, tales como China y Corea del Sur, se han prohibido ciertos tipos de transacciones en criptomonedas, mientras que otros países están trabajando para desplegar leyes y normas más claras[11].

En Colombia, la tecnología Blockchain viene ganando una mayor atención en los últimos años. El país ha experimentado un aumento en la aceptación de esta, especialmente en el sector financiero.

De igual manera se han creado startups basadas en Blockchain en Colombia, como la plataforma de pago en criptomonedas Bitso, que ha lanzado recientemente sus servicios en Colombia. De igual manera se han realizado varios eventos y conferencias relacionados con Blockchain, como lo fue la Cumbre mundial de Blockchain que se celebró en Bogotá en 2019.

En 2018, el Banco Central de Colombia anuncio que se encontraban explorando la posibilidad de utilizar Blockchain para la liquidación de pagos interbancarios. Además, la superintendencia financiera de Colombia ha establecido un grupo de

[10] “Ibid”, p. 27
[11] “Ibid”, p. 27

trabajo con el fin de explorar el uso de tecnologías de registro distribuido en el sector financiero. En cuanto a la regulación se ha adoptado un enfoque cauteloso hacía las criptomonedas y la tecnología. En el mismo año el gobierno emitió un comunicado en el que se indica que las criptomonedas no son una moneda en curso legal en el país y que no están respaldadas por el Banco de la República[12]

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

El Blockchain es una tecnología que tiene una base científica en criptografía, teoría de juegos, sistemas distribuidos y algoritmos de consenso.

- Criptografía: Para proteger y preservar la información que se intercambia en el Blockchain, se aplican métodos matemáticos que dificultan su alteración o falsificación. Estos métodos permiten encriptar las operaciones que se realizan y comprobar su veracidad y legalidad. Entre los métodos que se emplean están la función hash, la firma digital y el cifrado simétrico.
- Teoría de juegos: La tecnología Blockchain también es basada en un sistema de incentivos y desincentivos con el fin de motivar a los participantes a actuar de manera honestas. Esta teoría de juegos es usada para diseñar los algoritmos de consenso que son usados para validar las transacciones en la red, la teoría de juegos es usada también para modelar posibles escenarios de ataques en la red y con ello definir una mejor forma de defensa.
- Tecnología distribuida: El Blockchain funciona sin una entidad central que regule la red y en cambio, los nodos de la red colaboran para verificar las transacciones y para mantener una versión sincronizada del historial de transacciones.

[12] “Ibid”, p. 27

- Algoritmos de consenso: Los mecanismos de consenso son el corazón del Blockchain. Estos mecanismos se utilizan para verificar las transacciones y asegurar que todos los nodos de la red coincidan sobre el estado actual de la cadena de bloques. Los mecanismos de consenso más habituales son la prueba de trabajo (PoW) y la prueba de participación (PoS).

4.6 MARCO LEGAL

La historia clínica, es un documento médico legal, en el cual se registran datos de identificación y de procesos de la atención del paciente, de forma cronológica con los diagnósticos médicos y los procedimientos realizados por profesionales de la salud que intervienen en la atención.

Según resolución número 1995 de 1999 del Ministerio de Salud. Que la historia clínica es un documento de vital importancia para la prestación de los servicios de atención en salud y para el desarrollo científico y cultural del sector.[13]

Esta resolución es de obligatorio cumplimiento para todos los prestadores de servicios y demás personas jurídicas o naturales que se relacionen con la atención en el sector salud.

Articulo 3.- CARACTERISTICAS DE LA HISTORIA CLINICA

Integralidad: La historia clínica de un usuario debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención especifica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordando como un todo en sus

[13] MINISTERIO DE SALUD. RESOLUCIÓN NUMERO 1995 DE 1999 1995. (8, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clinica.

aspectos biológico, psicológico y social, e interrelacionando con sus dimensiones personal, familiar y comunitaria.

Secuencialidad: Los registros de la prestación de los servicios deben consignarse en la secuencia cronológica en que ocurrió la atención. Desde el punto de vista archivístico la historia clínica es un expediente que de manera cronológica debe acumular documentos relativos a la prestación de servicios de salud brindados al usuario.

Disponibilidad: Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la Ley.[14]

Articulo 9.- IDENTIFICACIÓN DEL USUARIO

Los contenidos mínimos de este componente son: datos personales de identificación de usuario, apellidos y nombres completos estados civil, documento de identidad, fecha de nacimiento, edad, sexo, ocupación, dirección y teléfono del domicilio y lugar de residencia, nombre y teléfono del acompañante; nombre teléfono y parentesco de la persona responsable del usuario, según el caso; aseguradora y tipo de vinculación.[15]

Articulo 14.- ACCESO A LA HISTORIA CLÍNICA

Podrán acceder a la información contenida en la historia clínica, en los términos previstos en la Ley:

- El usuario.
- El Equipo de Salud

[14] "Ibid", p. 26
[15] "Ibid", p. 26.

- Las autoridades judiciales y de salud en los casos previstos en la Ley.
- Las demás personas determinadas en la ley.

PARAGRAFO. El acceso a la historia clínica se entiende en todos los casos, única y exclusivamente para los fines que de acuerdo con la ley resulten procedentes, debiendo en todo caso, mantenerse la reserva legal[16]

Articulo 15.- RETENCIÓN Y TIEMPO DE CONSERVACIÓN

La historia clínica debe conservarse por un periodo mínimo de 20 años contados a partir de la fecha de la última atención. Mínimo cinco (5) años en el archivo de gestión del proveedor de servicios de salud y mínimo quince (15) años en el archivo central[17]

Articulo 16.- SEGURIDAD DEL ARCHIVO DE HISTORIAS CLÍNICAS

El prestador de servicios de salud debe archivar las historias clínicas en un área restringida, con acceso limitado al personal de salud autorizado, conservando las historias clínicas en condiciones que garanticen la integridad física y técnica, sin adulteraciones o alteraciones de la información.

Las instituciones prestadoras de servicios de salud y en general los prestadores encargados de la custodia de la historia clínica, deben velar por la conservación de la misma y responder por su adecuado cuidado.[18]

Articulo 18.- DE LOS MEDIOS TÉCNICOS DE REGISTRO Y CONSERVACIÓN DE LA HISTORIA CLÍNICA

[16] Ibid", p. 26.
[17] Ibid", p. 26.
[18] Ibid", p. 26.

Los programas automatizados que se diseñen y utilicen para el manejo de las Historias Clínicas, así como sus equipos y soportes documentales, deben estar provistos por mecanismos de seguridad, que imposibiliten la incorporación de modificaciones a la Historia Clínica una vez se registren y guarden los datos.

En todo caso debe protegerse la reserva de la historia clínica mediante mecanismos que impidan el acceso de personal no autorizado para conocerla y adoptar las medidas tendientes a evitar la destrucción de los registros en forma accidental o provocada[19]

Artículos 21.- SANCIONES

Los prestadores de salud que incumplan lo establecido en la presente resolución 1995 de 1999 historias clínicas, incurrirán en las sanciones aplicables de conformidad con las disposiciones legales vigentes.[20]

De igual manera en la Ley 1751 de 2015 también encontramos artículos afines con las historias clínicas.

Articulo 10.- DERECHOS Y DEBERES DE LAS PERSONAS, RELACIONADOS CON LA PRESTACIÓN DEL SERVICIO DE SALUD.

g) A que la historia clínica sea tratada de manera confidencial y reservada y que únicamente pueda ser conocida por terceros, previa autorización del paciente o en los casos previstos en la ley, y a poder consultar la totalidad de su historia clínica en forma gratuita y a obtener copia de la misma.[21]

[19] Ibid", p. 26.
[20] Ibid", p. 26.
[21] MINISTERIO DE SALUD Y DE LA PROTECCIÓN SOCIAL. LEY ESTATUTARIA N° 1751. (16, febrero, 2015). Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones.

Además, en Colombia, la Ley 1581 de 2012 establece las normas para la protección de datos personales, cuyo objetivo principal es proteger el derecho fundamental a la privacidad de las personas, estableciendo las reglas para el uso y tratamiento de la información personal. La ley establece los principios y obligaciones que deben seguir las empresas, entidades públicas y cualquier persona que maneje información personal de terceros

Principales aspectos de la Ley 1581 de 2012

- La definición de datos personales y la clasificación de estos
- La forma en que se deben recolectar, almacenar, usar y proteger los datos personales.
- La necesidad de obtener el consentimiento explícito de los titulares de los datos para su tratamiento
- La obligación de garantizar la seguridad de los datos personales y notificar de cualquier incidente de seguridad a los titulares
- El derecho de los titulares a conocer, actualizar y rectificar sus datos personales, así como a solicitar su eliminación en ciertas circunstancias
- Las sanciones y multas a las empresas o personas que incumplen la ley.

Artículo 5° Datos sensibles

Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido

político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.[22]

Para el gobierno de Colombia, es de suma importancia el impulso por la cuarta revolución industrial (4RI) es por esto por lo que aparecen en sus artículos la implementación de tecnologías emergentes que generen valor de lo público. La ley 1955 de 2019 de el Plan Nacional de Desarrollo definiendo que las entidades del orden nacional deben desarrollar planes de transformación digital

Artículo 147 TRANSFORMACIÓN DIGITAL PÚBLICA

Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros.[23]

Los proyectos estratégicos de transformación digital se orientarán por los siguientes principios:

6. Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios de Estado a través de nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data, inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares.[24]

[22] EL CONGRESO DE LA REPUBLICA. LEY ESTATUTARIA 1581 DE 2012. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales.
[23] EL CONGRESO DE COLOMBIA. Ley 1955 de 2019. (25, mayo, 2019). Por el cual se expide el plan nacional de desarrollo 2018-2022 pacto por colombia, pacto por la equidad.
[24] "Ibid"., p. 29.

9. Implementación de la política de racionalización de trámites para todos los tramites, eliminación de los que no se requieran, así como en el aprovechamiento de las tecnologías emergentes y exponenciales.[25]

Artículo 230 GOBIERNO DIGITAL COMO POLÍTICA DE GESTIÓN Y DESEMPEÑO.

Esta política liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones contemplará como acciones prioritarias el cumplimiento de los lineamientos y estándares para la integración de trámites al portal Único del Estado Colombiano, la publicación y el aprovechamiento de datos públicos, la adopción del modelo de territorios y ciudades inteligentes, la optimización de compras públicas de tecnologías de la información, la oferta y uso de software público, el aprovechamiento de tecnologías emergentes en el sector público, incremento de la confianza y la seguridad digital y el fomento a la participación y la democracia por medios digitales.[26]

5. EXAMINAR LOS TIPOS DE TECNOLOGÍA BLOCKCHAIN MEDIANTE UNA CARACTERIZACIÓN, CON EL FIN DE ESTABLECER LAS FUNCIONALIDADES DE CADA UNA DE ELLAS.

Con el propósito de contribuir a la digitalización del sector público y privado, el Ministerio de Tecnologías de la Información y Comunicación (TIC) de Colombia ha emitido la Guía de Orientación sobre Blockchain para la Incorporación y Ejecución de Proyectos en el Ámbito Estatal. El objetivo fundamental de esta guía es estimular a las entidades gubernamentales a adoptar la perspectiva de la Tecnología Gubernamental (GOVTECH) para promover iniciativas que impulsen la utilización de tecnologías emergentes.

[25] "Ibid".., p. 29.
[26] "Ibid"..., p. 29

La Guía de Orientación, destinada a la adopción e implementación de proyectos basados en la tecnología Blockchain en el entorno gubernamental colombiano, proporciona directrices que las entidades deben seguir para la ejecución exitosa de proyectos relacionados con esta tecnología innovadora en la administración pública.

Además, la guía tiene como propósito fomentar que las instituciones gubernamentales desarrollen e implementen proyectos de Blockchain bajo el marco del gobierno abierto. El gobierno abierto se caracteriza por abordar iniciativas con un enfoque en la transparencia, la rendición de cuentas y la promoción de la participación ciudadana en la gestión de asuntos públicos. Esto se realiza a través de planes de acción que ofrecen información detallada sobre la gestión gubernamental.

Este enfoque se sustenta en tres pilares fundamentales: la transparencia, que implica que las autoridades deben divulgar de manera accesible toda la información acerca de sus acciones y procesos en conformidad con las regulaciones establecidas; la colaboración, que promueve la cooperación entre la sociedad civil, las empresas y el gobierno; y la participación ciudadana, tanto directa como indirecta, que requiere un acceso efectivo a la información proporcionada por las instituciones gubernamentales.[27]

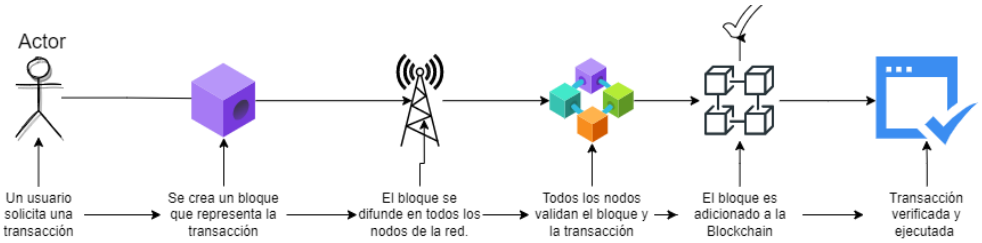
La tecnología Blockchain, también conocida como cadena de bloques, se define como un libro de contabilidad distribuido que actúa como un registro digital de acceso público, permitiendo que todos los interesados puedan verificar su contenido. En este registro, se registran de forma inmutable todas las transacciones realizadas por los usuarios.

[27] También disponible en PDF en: https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf

Estas transacciones se agrupan en paquetes de datos a los que se les asigna una marca de tiempo para determinar cuándo ocurrió cada transacción y prevenir la posibilidad de gastos duplicados. Cada uno de estos grupos de datos se conoce como "bloques."

Cabe destacar que los registros de datos en la cadena de bloques son inalterables, lo que significa que no pueden ser modificados ni eliminados. Los bloques se agregan de manera continua al registro, haciendo uso de un resumen digital de la información contenida en el bloque anterior.

Figura 2 Como funciona Blockchain .



Fuente: Propia

Es un sistema que permite la codificación de información para la transferencia de datos digitales, consigue ser ampliamente usada en las transacciones de bienes o servicios ya que una vez la información está en la cadena de bloques, la misma no puede ser borrada tan solo se permitirá añadir nuevos registros los cuales deben ser legitimados por la mayoría.

Blockchain es una tecnología que permite crear aplicaciones basadas en cadenas de bloques. Una de estas aplicaciones es Bitcoin, la divisa digital pionera y más conocida. No obstante, Blockchain no se limita al Bitcoin, sino que tiene muchas otras posibilidades.

A continuación, se presentan los atributos diferenciadores de la tecnología Blockchain:

Tabla 1 . Atributos de Blockchain

Atributos	Características Blockchain
Inmutabilidad en registros	En la tecnología Blockchain, los datos son almacenados de forma cifrada e irreversible, es decir, no pueden ser modificados ni alterados. Esto asegura la transparencia y la integridad de la información para las entidades y los beneficiarios de los procesos.
Seguridad de la información	Blockchain evita la pérdida de datos, incluso si hay fallas en la infraestructura tecnológica. Los datos se almacenan de manera cifrada y solo se puede acceder a ellos con el consentimiento del titular, asegurando una trazabilidad precisa de todas las interacciones registradas en la cadena de bloques.
Eliminación de intermediarios	La tecnología Blockchain permite que ciudadanos e instituciones interactúen directamente sin necesidad de intermediarios. Esto reduce la fricción y las demoras típicas asociadas con la intervención de terceros en las transacciones.
Trazabilidad	Blockchain ofrece una trazabilidad completa y detallada de cualquier información almacenada. Desde su registro inicial, cada evento relacionado con un dato puede ser seguido, lo que permite, por ejemplo, identificar plenamente la historia de un título de propiedad y las intervenciones legales sobre el mismo.
Base de Datos Descentralizada	A diferencia de otras tecnologías, Blockchain no depende de un único servidor o centro de datos, lo que proporciona una alta resiliencia a la información. Los registros distribuidos garantizan la inmutabilidad y la confiabilidad del sistema, superando las limitaciones de las bases de datos convencionales.

Fuente: Propia

Blockchain se puede considerar a prueba de falsificaciones e inmutables debido a la existencia de varios niveles de seguridad como lo son: Criptográfico, Descentralización, Consenso, Duplicación de datos. También, como el registro de las transacciones de la Blockchain se duplica en tantas copias como nodos tenga la red, por tal motivo para poder modificar el registro se hace necesario contar con más de la mitad de la potencia de cómputo de la red.

5.1 TIPOS DE BLOCKCHAIN

Desde el origen de Blockchain, se planteó como abierta y pública, planteando diferentes formas de solucionar problemas en las organizaciones al no depender de una entidad centralizada[28]

La primera generación de Blockchain tenía una limitación importante: no todas las empresas podían aprovechar una red pública, pues tenían información sensible que no podían compartir, ya que podría ser aprovechada por sus rivales. Esto motivó el desarrollo de cadenas de bloques con acceso restringido, es decir, redes Blockchain en las que la organización determina quién puede participar en ellas.

A continuación, se describen los tipos de Blockchain más comunes:

5.1.1 BLOCKCHAIN PÚBLICAS

En otras palabras, un público es una base de datos distribuida que cualquiera puede consultar, conectar y operar o colaborar en el mecanismo de consenso. Se le llama “sin permiso” porque los usuarios no tienen que revelar su identidad y todas las

[28] CALDERÓN, Christopher. Sector salud en la mira de los ‘hackers’: reportan 74 por ciento de incremento de ciberataques. El Financiero [página web]. (5, mayo, 2024). [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://www.elfinanciero.com.mx/empresas/2023/05/03/sector-salud-en-la-mira-de-los-hackers-reportan-74-por-ciento-de-incremento-de-ciberataques/>.

transacciones son visibles, no hay limitación de las cadenas de bloque cada par de la red de pares tiene una réplica[29]. Bitcoin y Ethereum son ejemplos notables de Blockchain públicos

La moneda digital “Bitcoin” es un conjunto de ideas y tecnologías de dinero electrónico que sirve para transferir valor entre los miembros de la red. Protocolo disponible como software libre, el cual puede ser instalado en diversos dispositivos[30]

Ethereum es otro caso de redes Blockchain públicas que se basa en una infraestructura computacional descentralizada a nivel mundial, de código abierto, en la que se ejecutan programas llamados Smart Contracts. Utiliza una cadena de bloques para sincronizar y guardar los cambios de estado del sistema, junto con una moneda virtual llamada “ether”, para medir y limitar los costos de los recursos de ejecución[31]

Las propiedades de las Blockchain públicas son:

No requieren de una entidad central de confianza, son redes libres, cualquier usuario puede incorporarse y participar en el consenso en las Blockchain públicas, son considerados sistemas totalmente descentralizados, son seguras, al emplear criptografía avanzada y claves privadas protegiendo las transacciones, e inmutables debido a que una vez el bloque de transacciones se agrega en la cadena no puede ser borrado o modificado.

[29] “Ibid”.., p. 45.
[30] “Ibid”.., p. 45.
[31] 2019 EL año de las blockchain federadas - Explicación simple de los consorcios de blockchains [Anónimo]. 101 Blockchains [página web]. [Consultado el 31, mayo, 2024]. Disponible en Internet: <https://101blockchains.com/es/blockchain-federadas/#5>.

Las transacciones no revelan la identidad de los usuarios, pero sí son transparentes, pues se comparten con los nodos que participan en la red una vez que se validan. La validación se realiza mediante métodos de consenso como las pruebas de trabajo o las pruebas de participación, que son ejecutadas por los propios nodos de la red.

La red Blockchain pública se basa en un mecanismo de consenso y no en intermediarios, al establecerse una red entre pares (P2P), lo que disminuye la probabilidad de que una persona o un grupo de personas dominen el sistema por completo.[32]

Todos los usuarios de la red Blockchain pública siguen los mismos protocolos de forma equitativa, lo que hace que la red no tenga puntos críticos o centralizados que puedan ser atacados por ciberdelincuentes, como ocurre en las redes centralizadas actuales.

5.1.2 BLOCKCHAIN PRIVADOS

Están bajo el dominio de una sola entidad o grupo que decide quién puede acceder a ellos, enviar operaciones en él y participar en el mecanismo de consenso[33]Los Blockchain privados responden a la demanda de organizaciones que quieren aprovechar la tecnología de cadena de bloques, pero que no pueden exponer sus datos, ya que son esenciales para el funcionamiento de la empresa y los datos deben mantenerse confidenciales.

[32] "Ibid".., p. 45
[33] "Ibid".., p. 46

Como los Blockchain privados están totalmente centralizados, son útiles como entornos de prueba. Quorum y Corda son ejemplos destacados de Blockchain privados.

Quorum es una Blockchain, desarrollada por JP Morgan, basada en Ethereum, enfocada en la empresa y su uso está orientado al sector bancario. Corda, al igual que Quorum, está dirigida al sector financiero, registra datos con el objetivo de fomentar un ambiente de red descentralizado. Además, gestiona contratos inteligentes y en cuanto a las transacciones, no las comparte con todos los nodos de la red, sino que las comparte con los nodos que tienen transacciones en común. De esta manera se preserva la privacidad entre las partes.

Las características de las Blockchain privados son:

Una organización es la encargada de regular la participación en la red, permitiendo o denegando el acceso a los individuos o entidades que lo soliciten, ya que existe una autoridad que supervisa toda la red.

Solo los miembros autorizados pueden acceder a los nodos de la red y realizar transacciones, lo que no implica que las Blockchain privadas carezcan de transparencia, confianza y seguridad entre los participantes seleccionados, sino que las hace redes muy eficientes, veloces en las transacciones y con costos de transacción reducidos.

Los participantes no tienen el anonimato que ofrecen las redes Blockchain públicas, ya que se requiere una autorización para ingresar al ecosistema. El rendimiento es superior, se efectúa un mayor número de transacciones por segundo en comparación con la Blockchain pública, es decir son más rápidas porque el número

de participantes es menor lo que conlleva que la red tarde menos en alcanzar el consenso.

5.1.3 BLOCKCHAIN SEMI-PRIVADA

Los Blockchain semiprivadas son operados por una sola organización quien le otorga acceso a cualquier usuario que cumpla los criterios preestablecidos, este tipo de Blockchain autorizado es atractivo en los casos de uso bussines-to-bussines (negocios dirigidos a empresas) y aplicaciones de gobierno.

Se debe tener en cuenta que los híbridos son los que combinan redes privadas y públicas. A su vez, pueden contar con operaciones en modo privado que eventualmente se registran en la red pública.

5.1.4 BLOCKCHAIN DE CONSORCIO

El proceso de consenso es controlado por un grupo preseleccionado, un grupo de instituciones. Se busca un punto intermedio entre Blockchain públicas y privadas, por ejemplo, el derecho a leer el Blockchain y enviarle transacciones puede ser público o restringido a los participantes. Los Blockchain de consorcio se consideran “Blockchain autorizados o federadas”. Por lo general, esta administrado por más de una entidad. Voltron se destaca por ser un ejemplo de Blockchain de consorcio.

Voltron es un proyecto impulsado por las empresas R3 y CryptoBLK y que recibe soporte técnico de Microsoft Azure, consiste en una red Blockchain de consorcio en la que participan doce bancos internacionales[34]

[34] 2019 EL año de las blockchain federadas - Explicación simple de los consorcios de blockchains [Anónimo]. 101 Blockchains [página web]. [Consultado el 31, mayo, 2023]. Disponible en Internet: <https://101blockchains.com/es/blockchain-federadas/#5>.

HSBC, BBVA, BNP Paribas, U.S Bank, SEB, Scotiabank, NatWest, Mizuho, Intesa Sanpaolo, ING, Bangkok Bank, and CTBC bank.

Usando la tecnología Blockchain de R3 para digitalizar toda la documentación oficial. La plataforma que están utilizando es Corda y la naturaleza descentralizada de esta para crear su plataforma federada.

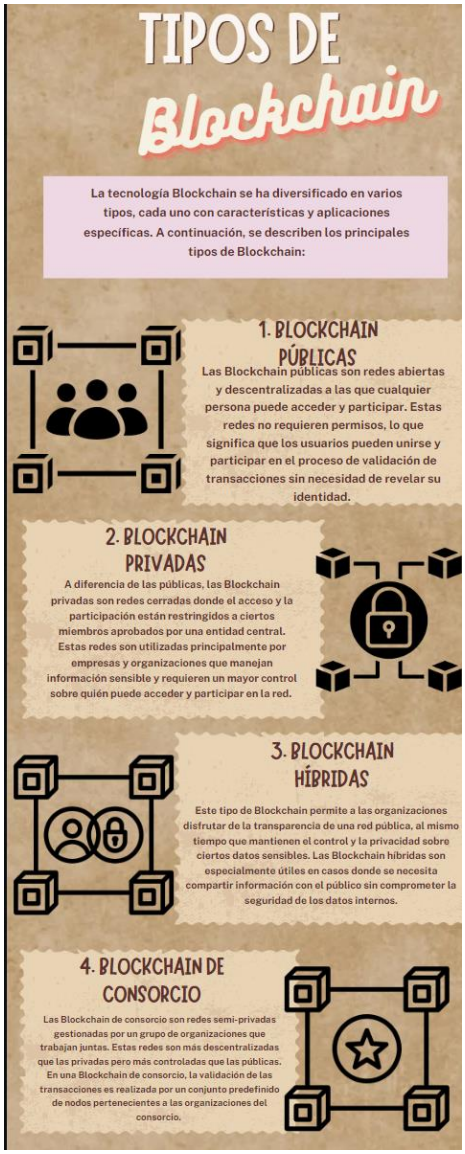
Las características de las Blockchain de consorcio son:

Las redes de cadena de bloques de consorcio integran las ventajas de las redes públicas y privadas, garantizando transparencia, confidencialidad y alta eficiencia sin que ninguna parte tenga poder de decisión.

Al tener menos participantes que una red pública, el mecanismo de consenso se basa en un sistema de votación, lo que permite una baja latencia y una mayor velocidad en la red.

Todos los nodos pueden leer y escribir transacciones, pero solo los nodos validadores pueden aprobarlas, los procesos de consenso están regulados por los seleccionados. Además, ningún nodo puede agregar un bloque a la cadena de bloques por su cuenta. Para ello debe someterse a votación (prueba de voto) en la que todos los nodos verifiquen y den su conformidad para que el bloque se incorpore a la cadena de bloques, asegurando que cada bloque sea válido y no contenga actividades ilícitas.

Figura 3 Tipos de Blockchain



Fuente: Propia

En resumen, el mecanismo de todas las redes Blockchain es muy parecido, se apoya en una red P2P (De par a par) con el objetivo de asegurar la descentralización y la comunicación entre los nodos de la red. Dentro de la red hay reglas y los algoritmos de consenso, los cuales se ocupan de buen funcionamiento de la cadena de bloques.

7. INVESTIGAR LOS RIESGOS ASOCIADOS A LAS HISTORIAS CLÍNICAS DEL SECTOR SALUD MEDIANTE UNA REVISIÓN BIBLIOGRÁFICA CON EL FIN DE DETERMINAR EL IMPACTO QUE PUEDAN TENER EN CASO DE PRESENTARSE UN INCIDENTE DE SEGURIDAD.

Los cibercriminales utilizan diversas técnicas para comprometer los sistemas del sector salud, tales como el phishing, el malware y los ataques de ransomware. Estas técnicas les permiten robar información personal y médica, bloquear servicios críticos e interferir o modificar historias clínicas.

De acuerdo con el Cyber Security Report 2023, se registraron 1463 intentos de ciberataques a hospitales, clínicas e instalaciones de investigación durante el año 2022, lo que representa un incremento del 74% respecto al año anterior[35]

El estudio también mostró que entre los grupos de ransomware que se han enfocado en atacar a organizaciones de atención medica se encuentran Lock Bit, Blackcat, Cuba, Zepelín, Conti y el recién desarticulado, Hive, que en enero pasado se reveló que habría afectado a más de mil 500 entidades, incluyendo hospitales, en más de 80 países.[36]

Latinoamérica es la tercera región del mundo con más ciberataques contra el sector salud, después de Europa central y Asia Oriental, ya que este sector es más

[35] LATINOAMÉRICA ES la tercera región con más ciberataques al sector salud [Anónimo]. Segurilatam [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://www.segurilatam.com/actualidad/ciberseguridad-latinoamerica-es-la-tercera-region-con-mas-ciberataques-al-sector-salud_20210109.html>.

[36] CALDERÓN, Christopher. Sector salud en la mira de los 'hackers': reportan 74 por ciento de incremento de ciberataques. El Financiero [página web]. (3, mayo, 2023). [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://www.elfinanciero.com.mx/empresas/2023/05/03/sector-salud-en-la-mira-de-los-hackers-reportan-74-por-ciento-de-incremento-de-ciberataques/>.

vulnerable a pagar por un rescate debido a la urgencia de mantener todos sus sistemas operativos[37]

Como lo revela el director de inteligencia de Datos de Check Point, Omer Dembinsky "el número de ciberataques a nivel mundial contra el sector salud ha experimentado un crecimiento exponencial. Está claro que los cibercriminales ven a los hospitales como objetivos que generan beneficios económicos, ya que acceden rápidamente a pagar para poder tener sus sistemas en funcionamiento"[38](Dembinsky, 2023)

La tecnología en Colombia ha traído muchos beneficios, pero también ha expuesto a las entidades a mayores riesgos de sufrir ciberataques que afectan su información y su funcionamiento. Estos ciberataques pueden generar pérdidas económicas y dañar la imagen de la organización[39]

El centro cibernético de la Policía Nacional informó que se recibieron 54.121 denuncias por ciberdelitos entre enero y octubre de 2022. Asimismo, la Policía Nacional de Colombia reportó que el sector salud fue víctima de al menos 104 ciberataques entre diciembre de 2022 y enero de 2023.[40]

Algunas organizaciones del sector salud sufrieron ataques cibernéticos, entre ellas Salud Total, Famisanar, Grupo Keralty (Sanitas y Colsanitas) y Audiofarma (Agencia Nacional de Ciberseguridad de Colombia, 2023).

---

[37] "Ibid".., p. 53

[38] LATINOAMÉRICA ES la tercera región con más ciberataques al sector salud [Anónimo]. Segurilatam [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://www.segurilatam.com/actualidad/ciberseguridad-latinoamerica-es-la-tercera-region-con-mas-ciberataques-al-sector-salud_20210109.html>.

[39] CASOS DE ciberataques: la salud peligra en colombia - keos.co [Anónimo]. keos.co [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://keos.co/casos-de-ciberataques-salud-colombia/>.

[40] "Ibid".., p. 54

La falta de capacidad tecnológica para operar en Salud Total implicó que los empleados tuvieran que permanecer en sus casas por varios días, así mismo durante este ciberataque los usuarios de esta entidad promotora de salud (EPS) no pudieron acceder a los servicios ofrecidos, como sus historias clínicas, tratamientos farmacológicos, consultas médicas, y otros

En Colombia Keralty que acoge a la EPS Sanitas y la empresa de medicina prepagada Colsanitas, operador de salud tuvo todos sus servicios virtuales tales como (la gestión de autorizaciones y el agendamiento de citas) fueron interrumpidos a finales de noviembre del año pasado.

Las historias clínicas son un documento fundamental en la atención médica y forman parte del expediente de los pacientes, contienen datos clasificados como sensibles que detalla sobre la salud del paciente, incluyendo antecedentes médicos e información personal, resultados de pruebas, diagnósticos, vida sexual tratamientos y datos relevantes, que sin un adecuado manejo pueden representar un riesgo para la privacidad y seguridad de los pacientes. A continuación, se relacionan los principales riesgos:

- Acceso no autorizado: El acceso no autorizado a las historias clínicas es uno de los principales riegos asociados a la privacidad y seguridad de los pacientes. Si los datos de la historia clínica están disponibles sin medidas de seguridad adecuadas, los datos pueden ser manipulados, robados o hasta utilizados para fines ilegales.
- Divulgación indebida: Las historias clínicas contienen información clasificada como sensible y privada sobre la salud de los pacientes. Si esta es divulgada indebidamente, puede llevar a consecuencias graves para los pacientes, como la discriminación, estigma y daño a su reputación.

- Pérdida o robo: Si las historias clínicas son robadas o se pierden, la información contenida en ellas puede caer en mano de ciberdelincuentes, colocando en riesgo la privacidad y el uso no autorizado a la información
- Errores de datos: Pueden traer consecuencias graves en la atención médica. Si la información contenida es errónea o incompleta, puede conllevar a diagnósticos erróneos, tratamientos inadecuados o incluso la muerte.
- Falta de actualización: Las historias clínicas deben ser actualizadas regularmente con el fin de garantizar que la información es precisa y efectiva.

Estos ciberataques intensificados en los últimos años en hospitales, clínicas, entidades promotoras de salud (EPS), instituciones prestadoras de servicios de salud (IPS), entidades de medicina prepagada etc. Son cada vez más frecuentes con consecuencias sumamente graves por la información sensible y confidencial que se maneja en estas entidades[41]

8. ANÁLISIS DE RIESGOS PRESENTES EN EL MANEJO DE HISTORIAS CLÍNICAS QUE PERMITA ESTABLECER EL TIPO DE BLOCKCHAIN MÁS ADECUADO PARA SU ASEGURAMIENTO

Los gobiernos pueden hacer uso de la tecnología Blockchain para ofrecer ciberseguridad, optimizar procesos, integrar servicios de forma “hiper-conectada” y así mismo robustecer la responsabilidad y confianza. Aprovechando una serie de aplicaciones en el sector público, incluyendo dinero digital, pagos, registro de tierras, gestión de identidad, trazabilidad se cadena de abastecimiento, salud, impuestos, votaciones entre otros.

[41] MINTIC RESPECTO a Blockchain : “Colombia tiene una oportunidad única de convertirse en un referente en la región [Anónimo]. Colombiafintech [página web]. [Consultado el 5, febrero, 2024]. Disponible en Internet: <https://www.colombiafintech.co/lineaDeTiempo/articulo/mintic-respecto-a-Blockchain -colombia-tiene-una-oportunidad-unica-de-convertirse-en-un-referente-en-la-region>.

Después de caracterizar la tecnología Blockchain y con el fin de concluir cual es el tipo (Publica, Privada o de Consorcio) más adecuado para el aseguramiento de las historias clínicas en el sector salud en Colombia los casos de éxito del mundo en organizaciones de esta industria, así mismo se destacarán sus ventajas y beneficios una vez implementada.

A continuación, se relacionan buenas prácticas internacionales en el uso de Blockchain en el sector salud.

Estados Unidos

La administración de Alimentos y Medicamentos (FDA) lanzó un proyecto piloto que explora la utilidad de Blockchain en el seguimiento seguro y la verificación de prescripciones médicas.[42]

Estonia

El programa e-Estonia tiene una identificación digital, con más de 700 millones de firmas digitales. El 99% de los datos de salud se digitalizan y almacenan en una cadena de bloques.[43]

El caso más representativo se encuentra en Estonia donde el sistema de salud se ha soportado en Blockchain, y su implementación se ha realizado en conjunto con la compañía Guardtime (2019), en esta Blockchain interactúan los ciudadanos, los prestadores de salud y las empresas aseguradoras del sector.[44]

[42] "Ibid", p. 30
[43] "Ibid", p. 30
[44] PAVA, Roberto; PEREZ CASTILLO, José Nelson y NIÑO VASQUEZ, Luis Fernando. Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y blockchain. En: Tecnura [en línea]. 1, enero, 2021. vol. 25, no. 67 [consultado el 26, mayo, 2023], p. 112-130. Disponible en Internet: <https://doi.org/10.14483/22487638.16159>. ISSN 2248-7638.

El uso de la tecnología Blockchain para un gobierno es prometedor y diverso, teniendo en cuenta que pueden funcionar como un gestor de información en la sociedad es por este motivo que se relacionan algunos ejemplos de aplicación en el sector salud en Colombia.

Los casos de uso en salud son muy diversos, uno de los más significativos s el de historias clínicas hasta la protección de la cadena de suministro de medicinas protegiéndolas contra la falsificación.[45]

También, existen proyectos cuyo fin es conectar a pacientes con doctores, por medio del uso de la tecnología Blockchain que manejan las PQRS (usando una inteligencia artificial), las citas de los especialistas y la base de datos de los afiliados haciendo más eficiente la gestión en salud, aumentando la contratación y médicos y mejorando los tiempos de atención a los pacientes.

Medicalchain: es una plataforma descentralizada que permite el intercambio y uso seguro, rápido y transparente de datos médicos. Haciendo uso de la tecnología Blockchain privada basada Hyperledger Fabric para crear una historia clínica electrónica basada en el usuario y mantener una única versión veraz de sus datos, garantizando la privacidad y la confidencialidad. Además, permitiendo a los usuarios dar acceso condicional a diferentes agentes sanitarios tales como médicos, hospitales laboratorios, farmacéuticos y aseguradoras para que interactúen según como consideren oportuno.

Hyperledger Fabric, es un proyecto de código abierto de Linux Foundatión bajo la plataforma de Blockchain empresarial de Hyperledger, es la infraestructura modular de Blockchain empresariales. Diseñada como base para desarrollar aplicaciones de nivel empresarial y soluciones sectoriales, la arquitectura modular y abierta utiliza

[45] “Ibid”, p. 30

componentes plug-and-play para acomodar una amplia gama de casos de uso. Con la participación de más de 120000 organizaciones y la colaboración de más de 15 000 ingenieros, Hyperledger Fabric ofrece un enfoque único para el consenso que permite el rendimiento a escala, al mismo tiempo que se respeta la demanda de privacidad de datos de las empresas[46]

Cada interacción con sus datos médicos es auditable, transparente y segura, y se registrara como una transacción en el libro mayor distribuido de Medicalchain. Durante este proceso, la privacidad del paciente está protegida en todo momento. La arquitectura basada en permisos, que permite distintos niveles de acceso: los usuarios controlan quien puede ver sus historiales, cuanto pueden ver y durante cuánto tiempo.

Medicalchain será una plataforma sobre la que se desarrollarán otras aplicaciones de salud digital; los usuarios podrán suscribirse a estas aplicaciones y servicios alimentados por sus datos sanitarios y protegidos por contratos inteligentes (Linux Foundatión, 2020).

Blockpharma: Los medicamentos falsificados y de baja calidad son responsables de provocar efectos adeversos en la salud de las personas. Además, los productos famaceuticos fraudulentos son responsables de crear enfermedades resistentes a los medicamentos. Una de las principales empresas de atención medica del Blockchain , blockpharma, ofrece una aplicación basada en Blockchain , que permite rastear la legitimidad de productos famacuticos.

Patientory: Es una plataforma de atención medica, sirve como herramienta vital para que los usuarios tomen control de su salud. Con apoyo en el cumplimiento de

[46] ¿QUÉ ES hyperledger fabric? | IBM [Anónimo]. IBM - Deutschland | IBM [página web]. [Consultado el 22, febrero, 2024]. Disponible en Internet: <https://www.ibm.com/es-es/topics/hyperledger>.

HIPAA, hace uso de una arquitectura Blockchain cuya finalidad es garatizar la descentralización de los datos de atención medica. Además, tambien garantiza salvaguardas contra violaciones de datos.

IRYO: Las redes iryo resuelven los problemas que surgen de los registros electrónicos medicos dispersos o EHR. Con la ayuda de la tecnología Blockchain , la red IRYO ayuda a alamcenar y conectar todos los EHR de forma descentralizada.

FarmaTrust: colabora con las principales empresas farmacéuticas siguiendo los marcos normativos internacionales. Proporciona mayor confiabilidad y transparencia en los registros de salud con soluciones basadas en Blockchain .

Los sistemas actuales de gestión de salud (Electronic health records -EHR-) no serán reemplazados por sistemas basados en Blockchain ; sino que se espera que estos se integren y coexistan para aprovechar los beneficios que ofrece esta tecnología.

A continuación, se presentan las ventajas de la aplicación de Blockchain en las historias clínicas para el sector salud en Colombia:

Seguridad en el Acceso a los Datos, la aplicación añade una capa extra de protección permitiendo el anonimato de los usuarios, y contando con procesos de validación y autenticación de pacientes legítimos verificados en la Blockchain .

Intercambio de Información Médica, al crear una única historia clínica por paciente facilita la comunicación entre médicos, enfermeros, especialistas, terapeutas, farmacéuticas; sin importar la localización geográfica donde se preste la atención.

Gobierno Digital, por ejemplo, como la aplicación de la Blockchain (e-Health records.) en Estonia que 2019 se lleva un registro de consultas o actualizaciones sobre las historias médicas.

Aplicaciones al sector salud

Datos clínicos. Con esta tecnología los historiales clínicos y datos médicos pueden ser leídos y compartidos con total certeza de su integridad. En cada fase de la transacción o consulta se tiene a disposición la 'trazabilidad del dato': podemos saber que ha ocurrido o ha sido aportado en su paso por cualquiera de los agentes (nodos) de la cadena.[47]

No existe un denominador común para el tipo de Blockchain utilizado en los trabajos analizados, aunque la mayoría prefieren Blockchain privada, en la que existe un mayor control sobre el registro, transmisión y consulta de datos. Por otro lado, existen soluciones que, por su complejidad o diseño, integran dos tipos diferentes de Blockchain, aprovechando los beneficios de cada uno de ellos.[48]

En conclusión y según la masa documental consultada para la elaboración de esta investigación el tipo de Blockchain más adecuado para el aseguramiento de las historias clínicas son las redes de cadena de bloques de consorcio ya que surgen como una solución para las entidades u organizaciones que quieren hacer públicos ciertos aspectos, mientras que otros se mantienen privados. Son una combinación entre las redes públicas y las privadas. Estas redes están descentralizadas, dado que estás que están controladas, generalmente, por más de una organización, en el caso de esta monografía a todas las entidades que hacen uso de historias clínicas a nivel nacional esto incluye a:

[47] BLOCKCHAIN, LA revolución en la gestión de nuestros datos de salud [Anónimo]. Elsevier Connect [página web]. [Consultado el 28, febrero, 2024]. Disponible en Internet: <https://www.elsevier.com/es-es/connect/ehealth/blockchain-aplicaciones-salud>.

[48] DULCE VILLARREAL, E. R., Betancourt Romo, J. H. ., Benavides Castillo, J. ., & Varón Guzmán , F. A. . (2022). Arquitectura Software de referencia para la gestión de la información de salud basada en tecnología Blockchain. Memorias. Recuperado a partir de https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4912

- Ministerio de Salud (Min Salud)
- Instituto Nacional de Salud (INS)
- Super intendencia de salud (Supersalud)
- Entidades Promotoras de Salud (EPS)
- Instituciones prestadoras de Servicios de Salud (IPS)
- Laboratorios diagnósticos
- Hospitales
- Clínicas
- Etc.

Estas organizaciones seleccionan a los nodos que pueden unirse a la red. Estos nodos no serán anónimos dado que se deben identificar para poder acceder a la red.

Las operaciones de consenso están controladas por los nodos preestablecidos. Con el fin de garantizar la funcionalidad adecuada, el consorcio tiene un nodo validador por cada organización participante que puede tanto validar transacciones, como iniciarlas o recibirlas. Mientras que los nodos miembros, en comparación, solamente pueden iniciar o recibir transacciones.

Este tipo de redes de consenso, como Voltron se basan en votaciones para poder agregar bloques a la cadena de bloques de la red. En las votaciones los nodos validadores deben alcanzar un consenso, puesto que bastará con que un nodo no esté de acuerdo para que el bloque no sea añadido en la cadena.

La tecnología Blockchain es una forma segura y confiable de almacenar y compartir información, y su aplicación en el sector salud de Colombia puede ser muy beneficiosa en términos de aseguramiento de la información de las historias clínicas.

Una de las ventajas de utilizar la tecnología Blockchain es que la información se almacena en una base de datos descentralizada y cifrada, lo que la hace mucho más difícil a los ciberdelincuentes corromperla. Además, cada transacción en la

cadena de bloques debe ser validada por múltiples nodos en la red, lo que garantiza que la información sea precisa y confiable.

En el sector salud de Colombia, esto podría traducirse en una mayor seguridad y privacidad para las historias clínicas de los pacientes, ya que los datos estarían protegidos contra ataques cibernéticos y otros riesgos de seguridad. Además, los pacientes tendrían un mayor control sobre sus datos médicos, ya que se podrían otorgar permisos específicos para que las partes interesadas o prestadores de servicios médicos accedan a su información, lo que se reflejaría en mejorar la seguridad y privacidad de la información médica en el sector salud lo que a su vez podría mejorar la calidad en la atención y consigo aumentar la confianza de los pacientes en el sistema de salud.

La integridad, la disponibilidad y la confidencialidad son conceptos clave en la seguridad de la información. Estos conceptos son particularmente relevantes en el contexto de la tecnología Blockchain, que se utiliza para registrar transacciones de forma segura y descentralizada.

La integridad se refiere a la calidad de la información que se almacena en un sistema. En el contexto de Blockchain, la integridad se refiere a la capacidad de garantizar que los datos almacenados en la cadena de bloques no han sido manipulados o alterados de ninguna manera. La tecnología Blockchain utiliza criptografía para garantizar la integridad de los datos almacenados en la cadena de bloques.

La disponibilidad se refiere a la capacidad de acceder a la información cuando se necesita. En el contexto de Blockchain, la disponibilidad se refiere a la capacidad de acceder a la información almacenada en la cadena de bloques en cualquier momento, desde cualquier lugar y por cualquier persona que tenga permiso para acceder a ella. La tecnología Blockchain utiliza una red distribuida para garantizar la disponibilidad de los datos almacenados en la cadena de bloques.

La confidencialidad se refiere a la capacidad de proteger la información de personas no autorizadas. En el contexto de Blockchain, la confidencialidad se refiere a la capacidad de proteger la información almacenada en la cadena de bloques de personas no autorizadas. La tecnología Blockchain utiliza criptografía para garantizar la confidencialidad de los datos almacenados en la cadena de bloques.

La tecnología Blockchain se utiliza para garantizar la integridad, la disponibilidad y la confidencialidad de los datos almacenados en la cadena de bloques. Estas características hacen que la tecnología Blockchain sea muy útil en una amplia variedad de aplicaciones, como las transacciones financieras, el seguimiento de la cadena de suministro y la gestión de la identidad digital.

Al utilizar Blockchain para almacenar y gestionar las historias clínicas de los pacientes, se pueden garantizar la privacidad y la seguridad de los datos, ya que la tecnología utiliza técnicas criptográficas para proteger la información y evitar el acceso no autorizado. Además, la descentralización de la información garantiza que los datos no estén centralizados en un solo lugar, lo que minimiza los riesgos de pérdida o manipulación de los datos.

La gestión de las historias clínicas a través de Blockchain también permite la interoperabilidad de los datos entre diferentes proveedores de atención médica, lo que facilita la transferencia de información entre hospitales, médicos y otros profesionales de la salud.

9. CONCLUSIONES

Con respecto al primer objetivo, he realizado una caracterización exhaustiva de los tipos de tecnología Blockchain disponibles en el mercado. Esta revisión detallada donde me permite comprender las funcionalidades inherentes a cada variante de Blockchain. Se ha identificado que existen múltiples enfoques, desde Blockchain públicos hasta Blockchain privados y consorcios, cada uno con sus ventajas y limitaciones. Esto proporciona una base sólida para seleccionar el tipo de Blockchain más apropiado en función de las necesidades específicas del sector salud.

En cuanto al segundo objetivo, la revisión bibliográfica ha revelado una serie de riesgos asociados a las historias clínicas en el sector salud. Estos riesgos incluyen la exposición de datos confidenciales, la manipulación no autorizada de registros médicos y la amenaza de incidentes de seguridad que podrían comprometer la privacidad y la integridad de la información médica. Esta comprensión de los riesgos es esencial para tomar decisiones informadas sobre la implementación de Blockchain, ya que nos permite evaluar cómo esta tecnología puede mitigar estos riesgos y fortalecer la seguridad de las historias clínicas.

Finalmente, el tercer objetivo se ha cumplido al analizar y comparar los tipos de Blockchain y los riesgos asociados a las historias clínicas en el sector salud. Por lo tanto; se ha logrado establecer una sólida base de conocimientos que nos permitirá seleccionar el tipo de Blockchain más adecuado para garantizar la seguridad y la integridad de las historias clínicas. Al considerar las funcionalidades de cada tipo de Blockchain en relación con los riesgos identificados, lo anterior permite estar dispuestos para tomar decisiones fundamentadas que respalden el aseguramiento de las historias clínicas en el sector salud.

10. RECOMENDACIONES

Los atributos de la tecnología Blockchain permitirán al paciente ejercer inspección sobre su historia clínica, generando de esta manera cambios en la forma de operar de las entidades de salud. Es importante sobresalir los atributos de la tecnología Blockchain donde permite al paciente ejecuta una revisión sobre su historia clínica lo cual podría generar ciertas inconformidades en las entidades de la salud.

Las entidades prestadoras de salud a nivel nacional deberán implementar y hacer uso de la tecnología Blockchain para garantizar la triada de la seguridad informática (Disponibilidad, integridad y confidencialidad) en las historias clínicas.

Los cambios que se prevén con implementación de la tecnología Blockchain en el sector salud pueden llegar a ser tan importantes para la sociedad, como lo fue la aparición de la world wide web en la década de los 90.

Esta tecnología ha empezado a transformar la forma de hacer transferencias digitales, creando nuevos valores digitales, tazando activos y certificando la información. Los cambios que se implementan en la tecnología Blockchain hacia el sector de la salud podría ser relevante para la sociedad, esta tecnología no solo transforma

11. BIBLIOGRAFÍA

2019 EL año de las Blockchain federadas - Explicación simple de los consorcios de Blockchain s [Anónimo]. 101 Blockchain s [página web]. [Consultado el 5, febrero, 2024]. Disponible en Internet: <https://101Blockchain s.com/es/Blockchain - federadas/#5>.

AMENAZA VS vulnerabilidad sabes se diferencian | empresas | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 5, febrero, 2024]. Disponible en Internet: <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>.

ANTONOPOULOS, Andreas M. y WOOD PH. D, Gavin. Mastering Ethereum: building smart contracts and daps. [s.l.]: O'Reilly Media, Inc., 2018. 424 p. ISBN 1491971894, 9781491971895.

Brennan, P. F., & Bakken, S. (2019). Blockchain for Electronic Health Records: Promising, But Caution Required. Oncology Nursing Forum, 46(5), 505-506. DOI: 10.1188/19.ONF.505-506

BLOCKCHAIN , LA revolución en la gestión de nuestros datos de salud [Anónimo]. Elsevier Connect [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://www.elsevier.com/es-es/connect/ehealth/Blockchain - aplicaciones-salud>.

BLOCKCHAIN , LA revolución en la gestión de nuestros datos de salud [Anónimo]. Elsevier Connect [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://www.elsevier.com/es-es/connect/ehealth/Blockchain - aplicaciones-salud>.

CALDERÓN, Christopher. Sector salud en la mira de los ‘hackers’: reportan 74 por ciento de incremento de ciberataques. El Financiero [página web]. (3, mayo, 2023). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.elfinanciero.com.mx/empresas/2023/05/03/sector-salud-en-la-mira-de-los-hackers-reportan-74-por-ciento-de-incremento-de-ciberataques/

CASOS DE ciberataques: la salud peligra en colombia - keos.co [Anónimo]. keos.co [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://keos.co/casos-de-ciberataques-salud-colombia/>.

Cointelegraph. (2023). Blockchain y tecnología P2P. Recuperado de https://cointelegraph.com/learn/what-are-peer-to-peer-p2p-Blockchain -networks-and-how-do-they-work

CLÚSTER DE software y TI, cámara de comercio de bogotá [Anónimo]. Cámara de Comercio de Bogotá [página web]. [Consultado el 5, febrero, 2024]. Disponible en Internet: <https://www.ccb.org.co/Clusteres/Cluster-de-Software-y-TI/Noticias/2019/Agosto-2019/Asi-va-el-negocio-de-Blockchain -en-Colombia>.

CLÚSTER DE software y TI, cámara de comercio de bogotá [Anónimo]. Cámara de Comercio de Bogotá [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: <https://www.ccb.org.co/Clusteres/Cluster-de-Software-y-TI/Noticias/2019/Agosto-2019/Asi-va-el-negocio-de-Blockchain -en-Colombia>.

EL CONGRESO DE COLOMBIA. Ley 1955 de 2019. (25, mayo, 2019). Por el cual se expide el plan nacional de desarrollo 2018-2022 pacto por colombia, pacto por la equidad.

EL CONGRESO DE LA REPUBLICA. LEY ESTATUTARIA 1581 DE 2012. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., Faxvaag, A., & Johannessen, L. (2019). Patients' Experiences of Accessing Their Electronic Health Records: National Patient Survey in Sweden. Journal of Medical Internet Research, 21(4), e12338. DOI: 10.2196/12338

HOME [Anonym]. Medicalchain [paginal web]. [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://medicalchain.com/en/>.

LATINOAMÉRICA ES la tercera región con más ciberataques al sector salud [Anónimo]. Segurilatam [página web]. [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.segurilatam.com/actualidad/ciberseguridad-latinoamerica-es-la-tercera-region-con-mas-ciberataques-al-sector-salud_20210109.html>.

Makhdoom, I., Abolhasani, M., & Burmeister, O. K. (2019). How Blockchain can Impact Healthcare: A Scoping Review. Journal of King Saud University - Computer and Information Sciences. DOI: 10.1016/j.jksuci.2019.01.041

MEDICALCHAIN. Medicalchain showcase video [video]. YouTube. (19, enero, 2018). [Consultado el 25, febrero, 2024]. 02:01 min. Disponible en Internet: <https://www.youtube.com/watch?v=cO-prfZBmyw>.

MINISTERIO DE SALUD. RESOLUCIÓN NUMERO 1995 DE 1999 1995. (8, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica.

MINISTERIO DE SALUD Y DE LA PROTECCIÓN SOCIAL. LEY ESTATUTARIA N° 1751. (16, febrero, 2015). Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones.

MINTIC RESPECTO a Blockchain : “Colombia tiene una oportunidad única de convertirse en un referente en la región [Anónimo]. Colombiafintech [página web]. [Consultado el 5, febrero, 2024]. Disponible en Internet: <https://www.colombiafintech.co/lineaDeTiempo/articulo/mintic-respecto-a-Blockchain -colombia-tiene-una-oportunidad-unica-de-convertirse-en-un-referente-en-la-region>.

ORTIZ CASAS, Camilo Andrés. Sistema seguro de manejo de historias clínicas con base en Blockchain . TESIS DE MAESTRÍA. Bogotá: Universidad de los Andes, 2020. 86 p.https://www.hornetsecurity.com/es/cyber-security-report/

Audifarma, Sanitas, Ciberataque en redes de salud en el manejo de los datos personales, 2023. https://audifarma.com.co/audifarma-sanitas/

PAVA, Roberto; PEREZ CASTILLO, José Nelson y NIÑO VASQUEZ, Luis Fernando. Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y Blockchain . En: Tecnura [en línea]. 1, enero, 2021. vol. 25, no. 67 [consultado el 26, mayo, 2023], p. 112-130. Disponible en Internet: <https://doi.org/10.14483/22487638.16159>. ISSN 2248-7638.

¿QUÉ ES Hyperledger Fabric? | IBM [Anónimo]. IBM - Deutschland | IBM [página web]. [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.ibm.com/es-es/topics/hyperledger>.

TOP HEALTHCARE Blockchain companies to watch in 2022 [Anonym]. 101 Blockchain s [página web]. [Consultado el 04, febrero, 2024]. Disponible en Internet: <https://101Blockchain s.com/healthcare-Blockchain -companies/>.